Quantum relative positioning in Hilbert space

Vittorio Giovannetti and Rosario Fazio

NEST-INFM & Scuola Normale Superiore, piazza dei Cavalieri 7, I-56126 Pisa, Italy.

A new class of state transformations that are quantum mechanically prohibited is introduced. These can be seen as the generalization of the universal-NOT transformation which, for all pure inputs state of a given Hilbert space produces pure outputs whose projection on the original state is fixed to a value smaller than one. The case of not pure output states is also addressed. We give an application of these transformations in the context of separability criteria.

Quantum mechanics imposes severe constraints on the way we can transform a physical system [1]. Perhaps the most popular of these quantum no-go theorems is related with the impossibility of cloning [2] an unknown quantum state $|\psi\rangle$. One cannot as well implement the Universal-Not (U-NOT) operation which transforms $|\psi\rangle$ into an orthonormal vector $|\psi_\perp\rangle$ [3, 4]. Along the same line we ask if it is possible to find universal operations that map an unknown state of a system S on a portion of the Hilbert space $\mathcal{H}_S$ of S such that some prescription is satisfied [5]. We refer to this question as the *Quantum Relative Positioning* (QRP) with respect to an unknown initial state. There are several motivations for addressing it. First of all the possibility to identify a new class of forbidden transformations which generalize the U-NOT operation allows us to frame what is known for the U-NOT in a broader context [1]. Moreover an analysis of the impossible QRP transformations may be relevant in the study of the entanglement. By definition the QRP transformations are in fact positive (they map quantum states of S into quantum states) but in general they will not be completely positive. Thus one may try to employ QRP operations for characterizing the entanglement of composite systems as in Refs. [6, 7, 8]: an example of this approach will be discussed at the end of the paper.

A complete characterization of the QRP transformations is quite a challenging task. In the following we will focus on an important class of these operations which contains the U-NOT as a special case. These are the *Generalized Quantum Movers* GQM(p) which transform an unknown input pure state $|\psi\rangle$ of S into some output density matrix ρ_p (possibly depending on $|\psi\rangle$) whose fidelity [9] with respect to $|\psi\rangle$ is equal to a fixed value $p < 1$, i.e.

$$F(|\psi\rangle, \rho_p) \equiv \langle \psi | \rho_p | \psi \rangle = p , \qquad (1)$$

for all $|\psi\rangle$ of $\mathcal{H}_S$ (the case $p = 1$ is trivially satisfied by the identity map). An important subset of the transformations GQM(p) is the set of the *Proper Quantum Movers* PQM(p) which satisfy Eq. (1) with pure outputs states $\rho_p = |\psi_p\rangle\langle\psi_p|$. More precisely, a proper quantum mover PQM(p) takes $|\psi\rangle$ into a pure vector $|\psi_p\rangle$ (depending on $|\psi\rangle$) whose projection $|\langle\psi|\psi_p\rangle|^2$ on $|\psi\rangle$ is equal to p. A simple geometrical representation of PQM(p) emerges in the case of qubits: here $|\psi_p\rangle$ is one of the points where
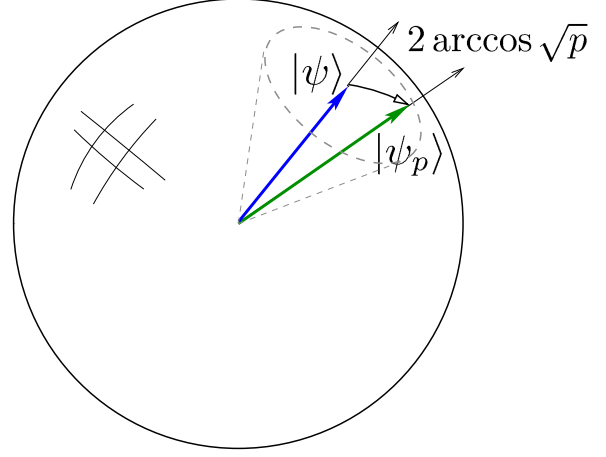

FIG. 1: Proper quantum mover PQM(p) on a qubit. This transformation takes an unknown state $|\psi\rangle$ of the qubit into a pure state $|\psi_p\rangle$ whose projection on the original vector is equal to p. Proper quantum movers should not be confused with ordinary rotations: the later are unitary transformations defined with respect to fixed external axis that do not depend on the input state $|\psi\rangle$. If $p < 1$ the transformation PQM(p) cannot be physically implemented, i.e. it cannot be obtained by means of unitary transformations acting on a (possible larger) Hilbert space [10]. For $p = 0$, PQM(0) performs a universal-not which maps $|\psi\rangle$ to its antipode.

the Bloch sphere intercepts the cone of angular opening $2\arccos\sqrt{p}$ originating from the center and oriented along $|\psi\rangle$ (see Fig. 1).

In the following we will prove the impossibility of building a machine which implements a proper quantum mover PQM(p) on a physical system S by showing that this transformation does not correspond to any linear, completely positive, trace preserving map [10] acting on the Hilbert space $\mathcal{H}_S$ of S. Since PQM(0) coincides with the U-NOT transformation, for $p = 0$ our results reproduce those of Refs. [3, 4]. However, the impossibility of implementing PQM(p) for $p \neq 0$ seems to be a novel quantum no-go theorem whose existence cannot be established from the impossibility of performing U-NOT (e.g. given the arbitrariness in selecting the output state $|\psi_p\rangle$, successive applications of PQM(p) on $|\psi\rangle$ do not necessarily produce a rotation of this state into an orthogonal vec-

tor). The scenario changes when the hypothesis on the purity of the output state is relaxed. In fact, we will show that GQM(p) with mixed outputs can be physically implemented on S if and only if p is greater than a threshold value $p_t(d)$ which depends upon the dimension d of the Hilbert space $\mathcal{H}_S$. Moreover a simple connection between the generalized quantum movers and the U-NOT will be established by showing that if the U-NOT were possible then also the GQM(p) could be also realized.

I. PURE OUTPUTS

Proving that proper quantum mover PQM(p) cannot be implemented on a physical system S is equivalent to showing the following:

Given $p \in [0, 1[$ there is no deterministic physical process $\mathcal{E}$ which transforms an unknown pure vector $|\psi\rangle$ of a generic Hilbert space $\mathcal{H}_S$ according to the mapping

$$|\psi\rangle \xrightarrow{\mathcal{E}} |\psi_p\rangle , \qquad (2)$$

where $|\psi_p\rangle$ is a pure state of $\mathcal{H}_S$ depending on $|\psi\rangle$ which satisfies the identity

$$|\langle \psi | \psi_p \rangle|^2 = p . \qquad (3)$$

The adjective "deterministic" in the hypothesis plays an important role. On one hand it allows us to exclude from the analysis those processes which implement (2) probabilistically, i.e. allowing some probability of failure. As in the case of the cloning and the U-NOT machines [3, 4, 8, 11] such transformations are not prohibited by quantum mechanics and the above no-go theorem does not apply to them. In addition the term "deterministic" indicates that here we are considering scenarios where the output state $|\psi_p\rangle$ associated with $|\psi\rangle$ is uniquely determined: i.e. if we run the transformation many times on various copies of a certain input $|\psi\rangle$, the output state will be always the same vector $|\psi_p\rangle$. This point is important since the vectors $|\psi_p\rangle$ which satisfy the property (3) form a dense subset of $\mathcal{H}_S$. A transformation (2) which randomly picks up one of these $|\psi_p\rangle$ is described by a GQM(p) map whose output state is not pure: these operations will be discussed in the next section where we will see that the possibility of implementing them depends explicitly on the dimension of $\mathcal{H}_S$.

The most general deterministic physical transformations (2) of the system S are the linear, completely positive, trace preserving (LCPT) maps $\mathcal{E}$ which for all $|\psi\rangle \in \mathcal{H}_S$ give

$$\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi_p\rangle\langle\psi_p| , \qquad (4)$$

with $|\psi_p\rangle$ unit vector of $\mathcal{H}_S$ such that Eq. (3) applies [12]. In the qubit case ($d = 2$) and for $p < 1/3$ the impossibility of implementing the transformation (4) can be established by considering the maximal fidelity achievable in performing an approximated U-NOT [3, 4]. In fact,

by expressing the trace of $\mathcal{E}(|\psi\rangle\langle\psi|)$ in the orthonormal basis $|\psi\rangle$, $|\psi_\perp\rangle$ of $\mathcal{H}_S$ we get

$$\langle\psi_\perp|\mathcal{E}(|\psi\rangle\langle\psi|)|\psi_\perp\rangle = 1 - p . \qquad (5)$$

The thesis then follows by observing that the left-hand side term of this expression is the fidelity of the output state of $\mathcal{E}$ with respect to the orthogonal vector $|\psi_\perp\rangle$ which according to [3, 4] is upper bounded by 2/3.

The above argument does not apply if $d > 2$ and for generic p. One can still prove that no transformations (4) exist by considering a unitary representation [10] of $\mathcal{E}$, i.e.

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \mathrm{Tr}_A\big[U \ (|\psi\rangle\langle\psi| \otimes |0\rangle_A\langle0|) \ U^\dagger \big] , \qquad (6)$$

where U is a unitary operator acting on S and on an ancillary system A, while $|0\rangle_A$ is a fiduciary state of A. According to Eq. (4) the pure states of $\mathcal{H}_S$ are mapped into pure states of the same space, this implies that the state $U |\psi\rangle \otimes |0\rangle_A$ cannot be entangled, i.e.

$$U |\psi\rangle \otimes |0\rangle_A = |\psi_p\rangle \otimes |\phi(\psi)\rangle_A \qquad (7)$$

with $|\phi(\psi)\rangle_A$ a pure state of A which, in principle, depends on the input state $|\psi\rangle$ of S. By applying this relation to the unit vector

$$|\psi\rangle = \alpha |k\rangle + \beta |k'\rangle , \qquad (8)$$

(with $|k\rangle$, $|k'\rangle$ orthonormal states of $\mathcal{H}_S$ and α, β complex such that $|\beta|^2 = 1 - |\alpha|^2$) and using the linearity of U one gets

$$|\psi_p\rangle \otimes |\phi(\psi)\rangle_A = \alpha |k_p\rangle \otimes |\phi(k)\rangle_A + \beta |k'_p\rangle \otimes |\phi(k')\rangle_A \qquad (9)$$

with $|k_p\rangle$, $|\phi(k)\rangle_A$ and $|k'_p\rangle$, $|\phi(k')\rangle_A$ defined as in Eq. (7). In particular $|k_p\rangle$ and $|k'_p\rangle$ are, respectively, the *unit vectors* of $\mathcal{H}_S$ which describes the outputs of the map $\mathcal{E}$ associated with $|k\rangle$, $|k'\rangle$: by hypothesis they satisfy the relations $\langle k_p|k\rangle = \sqrt{p}e^{i\phi}$, $\langle k'_p|k'\rangle = \sqrt{p}e^{i\phi'}$ for some phases ϕ and ϕ'. By projecting the left hand side of Eq. (9) on $|\psi\rangle$ we derive the following identity

$$\begin{aligned} p = \ & \|\big(|\alpha|^2\sqrt{p}\ e^{i\phi} + \alpha\beta^* \ \langle k'|k_p\rangle \ \big)|\phi(k)\rangle_A \\ & + \big(|\beta|^2\sqrt{p}\ e^{i\phi'} + \alpha^*\beta \ \langle k|k'_p\rangle \ \big)|\phi(k')\rangle_A\|^2 , \end{aligned} \qquad (10)$$

which must hold for all the complex amplitudes α and β. One can verify that this condition is satisfied if and only if

$$\langle k'|k_p\rangle = \langle k|k'_p\rangle = 0 , \qquad (11)$$

(see Appendix A for details). The impossibility of the transformation $\mathcal{E}$ finally follows by observing that Eq. (11) is in contradiction with $|k_p\rangle$ being a unit vector of $\mathcal{H}_S$. In fact since Eq. (11) applies for all $|k\rangle$ and $|k'\rangle$ orthonormal we have

$$\| |k_p\rangle \|^2 = |\langle k|k_p\rangle|^2 + \sum_{k'} |\langle k'|k_p\rangle|^2 = p , \qquad (12)$$

where the sum is performed over the set of vectors $\{|k'\rangle\}_{k'}$ which complete $|k\rangle$ to an orthonormal basis of $\mathcal{H}_S$. It should be stressed that the above derivation holds for all value of $p < 1$ and for Hilbert space $\mathcal{H}_S$ (also infinite-dimensional Hilbert spaces).

II. MIXED OUTPUTS

Consider now the case of generalized quantum movers GQM(p) with not necessarily pure output states ρ_b. These mappings include all those transformations which implement a proper quantum mover transformation (2) probabilistically, i.e. where the output state is randomly selected among the set of the vectors $|\psi_p\rangle$ which satisfies the condition of Eq. (3). Differently from the previous case, these generalized quantum movers are allowed at least for some restricted values of p. What is more interesting is that the generalized quantum movers GQM(p) can be implemented by means of LCPT maps only if p exceeds a threshold $p_t(d)$ which explicitly depends on d. Here we provide both upper and lower bounds for this threshold, i.e.

$$1/(2d - 1) \leqslant p_t(d) \leqslant 1/(d + 1). \quad (13)$$

Such bounds coincide for $d = 2$ so that $p_t(2) = 1/3$ and the threshold of the qubit case is completely determined by the above inequalities. As in the case of Eq. (5) this is a direct consequence of the 2/3 bound on the optimal fidelity associated with an approximate realization of a U-NOT [3, 4].

To derive the upper bound of Eq. (13) it is sufficient to provide a LCPT transformation that satisfies Eq. (1) for $p \geqslant 1/(d + 1)$. For instance let us analyze the linear mapping which takes any trace-class operator Λ of $\mathcal{H}_S$ to

$$\mathcal{N}(\Lambda) \equiv \frac{dp - 1}{d - 1}\Lambda + \frac{1 - p}{d - 1}\mathrm{Tr}[\Lambda]\,\mathbb{1}\,, \quad (14)$$

where $\mathbb{1}$ is the identity operator of $\mathcal{H}_S$. The transformation $\mathcal{N}$ belongs to the set of universal inverter super-operators that have been introduced in Refs. [7, 8] in the context of entanglement criteria for bipartite systems. Moreover, for $p = 1/(d + 1)$ Eq. (14) gives the approximated U-NOT mapping [3, 4, 11] which provides optimal output fidelity for $d = 2$ and, in the case $d > 2$, provides optimal fidelity in the class of LCPT maps which are covariant with respect to arbitrary unitary transformations of $\mathcal{H}_S$ [8]. One easily verifies that the transformation (14) satisfies the condition (1) for all $|\psi\rangle$. However, it turns out [8] that the map $\mathcal{N}$ is completely positive only for $p \geqslant 1/(d + 1)$ and this fixes the upper bound for the threshold $p_t(d)$. It should be stressed that in agreement with the no-go theorem on the deterministic quantum movers, the map $\mathcal{N}$ of Eq. (14) transforms pure states of $\mathcal{H}_S$ in mixed outputs. In fact, the purity of the output state is

$$\mathrm{Tr}\left[\,\mathcal{N}(|\psi\rangle\langle\psi|)^2\,\right] = \left(\frac{1 - p}{d - 1}\right)^2 + p^2,$$

which is strictly less than 1 for $p \geqslant 1/(d + 1)$ and $d \geqslant 2$.

To derive the lower bound of Eq. (13) assume that a LCPT map $\mathcal{E}$ satisfying Eq. (1) for all input states $|\psi\rangle$ exists. By applying this relation to the vector of Eq. (8) we get the following equation

$$
\begin{aligned}
p &= |\alpha|^2\langle k\,|\,\mathcal{E}(|\psi\rangle\langle\psi|)\,|k\rangle + |\beta|^2\langle k'\,|\,\mathcal{E}(|\psi\rangle\langle\psi|)\,|k'\rangle \\
&\quad + [\,\alpha\beta^*\langle k'\,|\,\mathcal{E}(|\psi\rangle\langle\psi|)\,|k\rangle + \mathrm{c.c.}\,]\,,
\end{aligned}
\quad (15)
$$

with

$$
\begin{aligned}
\mathcal{E}(|\psi\rangle\langle\psi|) &\equiv |\alpha|^2\mathcal{E}(|k\rangle\langle k|) + |\beta|^2\mathcal{E}(|k'\rangle\langle k'|) \\
&\quad + [\,\alpha\beta^*\mathcal{E}(|k\rangle\langle k'|) + \mathrm{h.c.}\,]\,.
\end{aligned}
\quad (16)
$$

Again by requiring Eq. (15) to hold for all α and β we get the following constraints on the map $\mathcal{E}$ which apply for all $|k\rangle$ and $|k'\rangle$ orthonormal

$$
\begin{cases}
2p = \langle kk'k'k\rangle + \langle k'kkk'\rangle + (\,\langle kkkk'\rangle + c.c\,) \\
\langle kk'kk'\rangle = 0 \\
\langle kkkk'\rangle + \langle kk'kk\rangle = 0\,,
\end{cases}
\quad (17)
$$

where we defined the quantities $\langle jk\ell m\rangle \equiv \langle j\,|\mathcal{E}(|k\rangle\langle\ell|)|m\rangle = \langle m\ell kj\rangle^*$ (see Appendix B). The previous equations can be supplemented by another constraint which can be obtained by applying $(\mathcal{E}_S \otimes \mathcal{I}_A)$ to the entangled state

$$|\Psi\rangle_{SA} \equiv \frac{1}{\sqrt{d}}\sum_{k=1}^{d} |k\rangle_S \otimes |k\rangle_A,$$

and requiring its trace to be properly normalized to 1 [In the above expression $\{|k\rangle_{S,A}\}_k$ are orthonormal bases of $\mathcal{H}_S$ and $\mathcal{H}_A$, respectively, and $\mathcal{I}_A$ is the identity mapping on the ancillary space $\mathcal{H}_A$]. This yields

$$1 = \frac{1}{d}\sum_{k=1}^{d}\sum_{k'=1}^{d}\langle k'kkk'\rangle = p + \sum_{k\neq k'}\langle k'kkk'\rangle/d\,, \quad (18)$$

where we used the hypothesis (1) to write $\langle kkkk\rangle = p$ for all $|k\rangle$. Equation (18) can be further simplified by replacing the first relation of the system (17). This gives

$$\sum_{k\neq k'}\langle kkk'k'\rangle = d(dp - 1).$$

The lower bound of Eq. (13) finally follows by comparing this relation with the inequality $|\langle kkk'k'\rangle| \leqslant p$, obtained by introducing a Kraus decomposition of the LCPT map $\mathcal{E}$ and applying the Cauchy-Schwarz inequality to the left hand side term [13].

We finally comment on the relations of GQM(p) with the U-NOT. One can easily verify that the set of the linear transformations which implement GQM(p) is closed under convex combination, e.g. given $\mathcal{E}_{p_i}$ LCPT implementations of GQM(p_i) on S and given $\{\lambda_i\}_i$ a set of probabilities, the transformation $\sum_i \lambda_i\mathcal{E}_{p_i}$ is a LCPT map which implements the generalized mover GQM(p)

on S with $p = \sum_i \lambda_i p_i$ being the average of the p_i's. This observation allows us to establish that if the U-NOT could be implemented through a LCPT transformation, then convex combinations of such a map and the identity map will implement the GQM(p) for $p < 1$.

III. QUANTUM MOVERS AND ENTANGLEMENT

In this last section we discuss an application of quantum movers in the context of entanglement witness. A central issue in quantum information is to determine whether or not a given density matrix R of a composite system S+A is entangled. The identification of classes of impossible transformations can become a powerful tool in this respect [6]. In our case, one can construct a one parameter set of positive *but* not completely positive linear maps $\{\mathcal{M}^{(p)}\}_p$ which implement the generalized quantum mover transformation GQM(p) on the system S. The presence of entanglement in R will then be detected by looking for the presence of negative eigenvalues in $\mathcal{M}_S^{(p)} \otimes \mathcal{I}_A(R)$ for some values of p. Moreover, one can use p as an effective "measure" of the entanglement in R as one expects intuitively only highly entangled states to feel the non complete positivity of the transformation $\mathcal{M}^{(p)}$ with $p \sim 1$. A suitable choice for the operators $\{\mathcal{M}^{(p)}\}_p$ is obtained by adding to the transformations (14) a linear term which gives null contribution to Eq. (1), e.g.

$$\mathcal{M}^{(p)}(\Lambda) \equiv \frac{dp-1}{d-1}\Lambda + \frac{1-p}{d-1}\text{Tr}[\Lambda]\,\mathbb{1} + i[\Lambda, \Theta] \quad (19)$$

with Θ being a Hermitian operator on $\mathcal{H}_S$. For the sake of simplicity let us consider the $d = 2$ case where we can select $\Theta = \sqrt{p(1-p)}\,\sigma_{\hat{n}}$ with $\sigma_{\hat{n}}$ being the Pauli operator along the $\hat{n}$ direction. With this choice Eq. (19) yields a mapping which, for all $p \in [0, 1[$ is positive but not completely positive (this can be verified for instance by a direct inspection of the corresponding Choi matrix [14]). As a test consider the set of Werner states [15]

$$R_q \equiv \frac{1-q}{4}\,\mathbb{1}_S \otimes \mathbb{1}_A + q\,|\Psi_-\rangle_{SA}\langle\Psi_-|\,, \quad (20)$$

which have concurrence [16] $C = \max\{0, (3q-1)/2\}$ and are hence separable if and only if $q \leqslant 1/3$ [in the above expression $|\Psi_-\rangle = (|01\rangle_{SA} - |10\rangle_{SA})/\sqrt{2}$ is the singlet state]. The eigenvalues of $\mathcal{M}_S^{(p)} \otimes \mathcal{I}_A(R_q)$ can be easily computed: three of them are always positive and the fourth is equal to

$$\lambda(q, p) \equiv q(p - (3q-1)/2q)/2\,. \quad (21)$$

For R_q separable (i.e. $q \leqslant 1/3$) this quantity is positive for all p. However for R_q entangled (i.e. $q > 1/3$) $\lambda(q, p)$ is negative for all p smaller than the critical value $(3q-1)/2q = (3/2)[1 - 1/(2C+1)]$ which monotonically

increases with C. As intuitively expected the more entanglement is in R_q the more transformations $\mathcal{M}_S^{(p)} \otimes \mathcal{I}_A(R_q)$ are able to detect it.

IV. CONCLUSIONS

We have introduced a new class of impossible quantum operations, the quantum movers which include, as a special case, the U-NOT transformation of Refs. [3, 4]. We proved that it is not possible to transform an unknown state $|\psi\rangle$ of a system S under the requirement that the final output configuration $|\psi_p\rangle$ has a fixed (non unitary) component along the direction of the initial state. By relaxing the requirement on the purity of the final configuration of the system, there exists a threshold $p_t(d)$ for the value of the input-output fidelity above which mixed quantum movers can be implemented. We related the movers to the U-NOT and we showed an application of these transformation in the context of separability criteria. The approach introduced in this work can be further extended. One can, for example, analyze the case in which the output fidelity of a quantum mover is bounded in a given interval, e.g. $F \in [p_1, p_2]$. Moreover, as in the case of a U-NOT transformation, it may be interesting to analyze under which conditions the GQM(p) with p below the threshold value $p_t(d)$ can be realized approximatively.

APPENDIX A

Here we show that if Eq. (10) applies for all the complex amplitudes α and β then the constraint (11) must be satisfied. For ease of notation define $\eta_1 \equiv \langle k' | k_p \rangle$, $\eta_2 \equiv \langle k | k'_p \rangle$ and $h \equiv {}_A\langle \phi(k') | \phi(k) \rangle_A$ and call $F(\alpha, \beta)$ the function at the right hand side of Eq. (10). According to this equation $F(\alpha, \beta)$ is equal to p for all values of α and β. Consequently we can write

$$\begin{cases} F(\alpha, \beta) - F(\alpha, -\beta) = 0 \\ F(\alpha, \beta) + F(\alpha, -\beta) - F(\alpha, i\beta) - F(\alpha, -i\beta) = 0 \end{cases} \text{(A1)}$$

When considered for generic α, β and for $p \neq 0$ the above system reduces to

$$\begin{cases} \eta_1\,\eta_2^*\,h = 0 \\ \eta_1 + \eta_2^*\,h = 0 \\ \eta_2 + \eta_1^*\,h = 0\,, \end{cases}$$

which has solution $\eta_1 = \eta_2 = 0$ independently from the value of h. This proves that Eq. (10) implies Eq. (11) for $p \neq 0$. For $p = 0$ we replace Eq. (A1) with

$$F(\alpha, \beta) + F(\alpha, i\beta) = 4|\alpha\beta|^2(|\eta_1|^2 + |\eta_2|^2) = 0\,.$$

which, again, holds for all α and β if and only if $\eta_1 = \eta_2 = 0$.

APPENDIX B

Here we show that if Eq. (15) applies for all the complex amplitudes α and β, then the constraints (17) must be satisfied. Consider the right hand side term of Eq. (15). By using Eq. (16), this can be explicitly written as,

$$
\begin{aligned}
G(\alpha, \beta) \equiv\ & (|\alpha|^4 + |\beta|^4)p/2 \\
& + |\alpha^3\beta|(e^{i\theta}\langle kkkk'\rangle + e^{-i\theta}\langle kkk'k\rangle) \\
& + |\alpha\beta^3|(e^{-i\theta}\langle k'k'k'k\rangle + e^{i\theta}\langle k'k'kk'\rangle) \\
& + |\alpha\beta|^2(\langle kk'k'k\rangle + \langle kkk'k'\rangle + e^{2i\theta}\langle kk'kk'\rangle) \\
& + \text{c.c.}
\end{aligned}
\tag{B1}
$$

where $\theta \equiv \arg(\alpha^*\beta)$ is the relative phase of β and α. According to Eq. (15) the function $G(\alpha, \beta)$ is constant and equal to p for all values of the amplitudes α and β. The constraints of Eq. (17) then follows by studying the Fourier components of (15) with respect to the phases $0, \pm\theta$ and $\pm 2\theta$, or equivalently by considering the following identities

$$
\begin{aligned}
G(\alpha, \beta) + G(\alpha, -\beta) + G(\alpha, i\beta) + G(\alpha, -i\beta) &= 4p \\
G(\alpha, \beta) + G(\alpha, -\beta) - G(\alpha, i\beta) - G(\alpha, -i\beta) &= 0 \\
G(\alpha, \beta) - G(\alpha, -\beta) &= 0 \ .
\end{aligned}
$$

ACKNOWLEDGMENTS

[1] R. F. Werner, *Quantum Information Theory – an Invitation* in Springer Tracts in Modern Physics Vol. 173, (Springer-Verlag, Telos, 2001), p. 14.

[2] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[3] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[4] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, R2626 (1999); V. Bužek, M. Hillery, and R. F. Werner, J. Mod. Opt. **47**, 211 (2000).

[5] For instance the fidelity F among the input ρ_{in} and the output state ρ_{out} of the transformation should fulfill predefined constraints, e.g. $p_1 \leqslant F \leqslant p_2$ with the parameters p_1 and p_2 independent from ρ_{in}.

[6] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[7] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[8] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).

[9] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994); A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[11] F. De Martini, V. Bužek, F. Sciarrino, and C. Sias, Nature **419**, 815 (2002).

[12] The trace decreasing operation of $\mathcal{H}_S$ describes non-deterministic processes which are excluded from the analysis by hypothesis.

[13] Let $\{M_\ell\}_\ell$ be a Kraus set of $\mathcal{E}$, such that $\mathcal{E}(\Lambda) = \sum_\ell M_\ell \Lambda M_\ell^\dagger$ [10]. Then using the Cauchy-Schwarz inequality we have

$$
\begin{aligned}
|\langle kkk'k'\rangle| &= |\sum_\ell \langle k|M_\ell|k\rangle\langle k'|M_\ell^\dagger|k'\rangle| \\
&\leqslant \sqrt{\sum_\ell |\langle k|M_\ell|k\rangle|^2 \ \sum_\ell |\langle k'|M_\ell|k'\rangle|^2} \\
&= \sqrt{\langle kkkk\rangle\langle k'k'k'k'\rangle} = p \ .
\end{aligned}
$$

[14] M. D. Choi, Lin. Alg. Appl. **10**, 285 (1975).

[15] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[16] W. K. Wootters, Phys. Rev. Lett. **80** 2245 (1998).